UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/581,064	10/07/2002	Ahmet Mursit Eskicioglu	RCA88783	6883

7590 06/30/2004

Joseph S Tripoli
Thomson Multimedia Licensing Inc
PO Box 5312
Princeton, NJ 08540

EXAMINER	
KLIMACH, PAULA W	

ART UNIT	PAPER NUMBER
2135	16

DATE MAILED: 06/30/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	09/581,064	ESKICIOGLU ET AL.
	Examiner	Art Unit
	Paula W Klimach	2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 April 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-7* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-7* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *14*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

This office action is in response to amendment filed on 4/19/04 (Paper No. 15). Original application contained Claims 1-7. Applicant amended Claims 1 and 5. The amendment filed on 4/19/04 have been entered and made of record. Therefore, presently pending claims are 1-7.

Response to Arguments

Applicant's arguments filed 4/19/04 have been fully considered but they are not persuasive because of following reasons.

Applicant argued, "Chaney fails to teach the limitation of generating the scrambling key based on a first seed value received in the smart card and a second seed value being permanently stored in the smart card". This is not found persuasive. A key value is the equivalent to the seed. The examiner agrees with the applicant that Chaney does not disclose the key based on the first seed value received in the smart card. However, Chaney discloses a key that is permanently stored in the smart card (column 10 lines 60-67). Santis discloses function sharing, which is the equivalent to key sharing. Sharing the function indicates that in the combination of Chaney and Santis the card as disclosed by Chaney would receive the information that would enable the card to share the function (key) as in the function sharing disclosed by Santis and thereby facilitating the function reconstruction (Santis, Section 3, pages 524 and 525).

Therefore, the examiner asserts that Santis does teach the subject matter broadly recited in independent Claims 1 and 5. Dependent Claims 2-4, and 6-7 are also rejected at least by virtue of their dependency on independent claims and by other reason set forth in this office action (Paper No. 16). Accordingly, rejections for claims 1-7 are respectfully maintained.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

1. **Claims 1-8** are rejected under 35 U.S.C. 103(a) as being unpatentable over Chaney (6,035,037) in view of Santis et al.

In reference to claim 1, Chaney discloses a method for managing access to a signal representative of an event of a service provider, said method comprising:

Receiving said signal in a smart card, said signal being scrambled using a scrambling key (column 4 lines 18-21). Therefore a key that is permanently stored in the smart card.

Descrambling, in said smart card, said signal using said generated scrambling key to provide a descrambled signal (column 3 lines 8-21).

Although Chaney teaches the generation of a scrambling key (column 7 lines 11-13) and the storage of an algorithm in the smart card, the reference does not explicitly express key based on a first seed value received in said smart card and a second seed value; and receiving, in said smart card, data representative of a first seed value.

Santis discloses generating said scrambling key using said first seed value received in said smart card and a second seed value, (page 528 Protocol 2 Part Shadow function generation phase); and receiving, data representative of a first seed value (page 528 Protocol 2 shared function evaluation phase).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to generate the scrambling key (function) by function sharing as disclosed by Santis in the smart card as disclosed by Chaney using the key that is permanently stored in the card. One of ordinary skill in the art would have been motivated to do this because the need for shareable functions is required to distribute the functionality of a party performing cryptography (page 522 Introduction). It would enable a message to be broadcast and only a select subset of listeners.

In reference to claim 5, Chaney discloses a system for managing access between a service provider and a device having a smart card coupled thereto, said device performing the steps of:

Receiving from the service provider a signal representative of an event, said signal being scrambled using a scrambling key (column 4 lines 18-21).

Receiving from the service provider data representative of descrambling data from the ECM packet (column 7 lines 1-15).

Receiving from the smart card the descrambled signal (column 6 lines 7-16). Chaney also discloses a system where the software, and therefore the algorithm, for descrambling data is stored within the smart card and the algorithm uses the generated descrambling key (column 7 lines 1-15). , said smart card having a means for access control processing (column 7 lines 30-35).

Chaney does not expressly discloses the descrambling data received in the form of a first seed value which is selected form a Euclidean plane.

However, Santis discloses receiving from the service provider data, representative of a first seed value, said first seed value being selected from a Euclidean plane (page 528 Protocol 2 in

combination with Definition 6). Further Santis discloses coupling said scrambled signal and said first seed value, both received from the service provider, to said smart card; means for generating said scrambling key by calculating the Y-intercept -. of a line on said Euclidean plane by said first seed value and a second seed value which is permanently stored [, said second seed value being pre-stored] in said smart card and means for descrambling, within said smart card, said signal using said generated scrambling key to generate a descrambled signal (Page 524 part 3.1).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to generate the scrambling key as disclosed by Santis in the smart card as disclosed by Chaney. One of ordinary skill in the art would have been motivated to do this because the need for shareable functions is required to distribute the functionality of a party performing cryptography (page 522 Introduction). It would enable a message to be broadcast and only a select subset of listeners.

2. Claims 2-4, and 6-8 are rejected as in claims 1 and 5 respectively above.

In reference to claim 2, wherein said first and second seed values are 20 points on a Euclidean plane. The definition indicates that the Euclidean algorithm is implemented and therefore it can be assumed that the Euclidean space is used. The number of points chosen is a design decision.

In reference to claim 3, wherein the step of generating said scrambling key comprises calculating the Y-intercept of a line formed on said Euclidean plane by said first and second seed values (Santis page 524 part 3.1).

In reference to claim 4, wherein said smart card has a card body having a plurality of terminals arranged on a surface of said card body in accordance with one of 150 7816 and PCMCIA card standards (Chaney column 7 lines 36-50 in combination with Fig. 2A).

In reference to claim 6, wherein the device is a set-top box. It is obvious that the device the smart card is connected to in Fig. 1 is a set-top box, since this is a well-known method of receiving scrambled video data.

In reference to claims 7 and 8, wherein the device is a digital television or a digital videocassette recorder. It is well know that the video signal sent form Fig. 1 part 150 and 155 is sent to a display. A digital television is one type of display. The type of display chosen is a design decision. A digital videocassette recorder is also well known in the art for video recording and viewing.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paula W Klimach whose telephone number is (703) 305-8421. The examiner can normally be reached on Mon to Thr 9:30 a.m to 5:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (703) 305-4393. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

PWK
Friday, June 25, 2004

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100